UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,117	01/28/2002	Anthony J. Wiley	60006751-2	2629

7590 09/29/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/056,117	WILEY ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/28/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on January 28, 2002 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Wiegley, U.S. Patent 6,711,677.

As per claim 1, it is taught by Wiegley of a printer device comprising: a data input device for receiving an encrypted digital document file; a decryption algorithm for decrypting said received document file; a controller for controlling printing of an image

of data contained in said received document file; and a printer mechanism for printing a physical copy of said document file, wherein said controller operates to control printing of a predetermined quantity of said physical copy, and after printing of said physical copy, automatically deletes said electronic document file from said memory (col. 1, line 60 through col. 2, line 13).

As per claim 2, Wiegley discloses of a decryption key locally stored in said printer device (col. 2, lines 29-34).

As per claim 3, Wiegley teaches of a network interface for receiving said encrypted digital document file over a network (as shown in Figure 2 as items #14 and #42).

As per claim 4, it is disclosed by Wiegley that the controller stores a unique device identification data uniquely identifying said printer device, said controller operating to compare a received unique identifier data contained in said received document file with said stored unique device identifier; and if said received unique device identifier data differs from said stored unique device identifier data, delete said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 5, Wiegley teaches that the controller stores a unique device identification data uniquely identifying said printer device, said controller operating to: compare a received unique identifier data contained in said received document file with said stored unique device identifier; and if said received document identification data is identical to said received unique device identifier data, control said print mechanism to

print at least one said physical copy of said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 6, it is taught by Wiegley that the controller operates to read a quantity permission data content of said document file, said quantity permission data specifying a number of authorized copies of said document file to be printed; and said controller controls said printer mechanism such that said permitted quantity of physical copies of said document file are printed (col. 4, lines 30-46).

As per claim 7, the teachings of Wiegley disclose that the controller operates to generate a confirmation message confirming receipt of said document file (col. 1, lines 12-26).

As per claim 8, it is disclosed by Wiegley that the controller operates to generate a confirmation message confirming receipt of said document file; said confirmation message comprises a time and date data, specifying a time and date of receipt of said document file and a number of copies printed data, specifying a number of copies of said document file physically printed by said print mechanism (col. 1, lines 12-26 and col. 4, lines 30-46).

As per claim 9, Wiegley teaches of a printer device comprising: a data input device for receiving an encrypted digital document file; a decryption algorithm for decrypting said received document file; a controller for controlling printing of an image of data contained in said received documents file; and a printer mechanism for printing a physical copy of said document file, wherein said controller operates to check a unique device identification data contained in said document file with a stored unique

device identification data of said printer device, and provided a successful match is found, print said physical copy of said document file; and if said received unique device identifier differs from said stored unique device identifier data, said controller operates to delete said document file without printing a physical copy of said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 10, it is disclosed by Wiegley of a computer entity configured for sending secure encrypted document files, said computer entity comprising: a data processor; a memory; an encryption algorithm capable of encrypting a document file; a device selector for selecting a said uniquely identifiable recipient device; a file selector for selecting a document file; a stored list of a set of authorized recipient devices, each said recipient device identified by a unique device identifier data inaccessibly embedded within said computer entity; wherein said computer entity operates to: select at least one document file; select at least one said uniquely identifiable recipient device to send said document to; encrypt said document files; and address said at least one document file to said selected uniquely identified recipient device (col. 1, line 60 through col. 2, line 13; col. 2, lines 35-53; and col. 3, lines 50-56).

As per claim 11, it is taught by Wiegley of a network interface capable of sending said document file over a network to said selected recipient device (col. 2, lines 29-34).

As per claim 12, Wiegley discloses of a user interface capable of displaying a history list of document files sent, said history list comprising data describing a document file sent; data describing at least one said recipient device to which said

document file has been sent; data describing a number of copies of documents said recipient device is authorized to print from said received document file (col. 4, lines 30-46).

As per claim 13, the teachings of Wiegley disclose that the user interface further displays data describing an encryption method used for sending said document (col. 4, line 46 through col. 5, line 24).

As per claim 14, Wiegley discloses of that the user interface displays an acknowledgement message data describing receipt of said document file by a said recipient device (col. 1, lines 12-26).

As per claim 15, it is taught by Wiegley of a distributed secure document printing system, said system comprising at least one sending computer entity, capable of sending an encrypted electronic document file, said document file having an encrypted data content, and a unique device identifier data identifying a recipient printer device to which said document file is intended to be printed by; and at least one recipient printer device, said recipient printer device capable of receiving said encrypted document file, establishing that said document file is intended for said recipient printer device, decrypting and printing said document file, and automatically deleting said electronic document file after printing a physical copy of a document from said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 16, the disclosure of Wiegley teaches that the recipient printer device is capable of reading a permitted quantity data content of said document file;

and said recipient printer device operates for printing a number of physical copies of said document file, corresponding to the permitted quantity data (col. 4, lines 30-46).

As per claim 17, Wiegley teaches that the recipient printer device is configured to send a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file (col. 4, lines 30-46).

As per claim 18, Wiegley discloses of a method of securely communicating an electronic document file over a network, said method comprising the steps of: encrypting said document file; specifying a recipient device for sending said document file to, said recipient device being uniquely identifiable by a unique device identifier data; attaching said unique identifier data to said document file; sending said document file in encrypted format to said intended recipient device; receiving said transmitted document file and decrypting said document file; reading said unique device identifier data of said document file; if said unique device identifier data of said document file corresponds to a unique device identifier data of said recipient device, printing a physical copy of said document file; and if said unique device identifier data of said document file does not correspond with said unique device identifier data of said recipient device, deleting said received document file without printing a physical copy of said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 19, Wiegley teaches that after printing said physical copy, deleting said electronic document file from said recipient device (col. 2, lines 10-13).

As per claim 20, it is disclosed by Wiegley of specifying a permitted quantity of physical copies of said document file to be printed and printing said permitted number of copies of said document file (col. 4, lines 30-46).

As per claim 21, Wiegley teaches of a method of secure printing of a received document file, said method comprising the steps of receiving said document file in encrypted format at a receiving device; decrypting said document file; reading a unique device identifier data identifying a recipient device for which said document file is intended; comparing said unique device identifier data with a locally stored device identifier data stored at said receiving device; if said received unique device identifier data corresponds with said locally stored device identifier data, printing at least one physical copy of said document file; if said received unique device identifier data differs from said stored unique device identifier data, deleting said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 22, Wiegley discloses of deleting said electronic document file, after printing said physical copy of said document file (col. 2, lines 10-13).

As per claim 23, in the disclosure of Wiegley, it is taught the step of reading a permitted quantity data describing a permitted quantity of copies of said document file; and printing said permitted quantity of copies of said document file (col. 4, lines 30-46).

As per claim 24, Wiegley teaches that the document file, after decryption is prevented from being viewed on a visual display device prior to printing (col. 4, line 46 through col. 5, line 24).

As per claim 25, Wiegley discloses that the document file is received via an intermediary carrier device having data storage capability (col. 3, lines 41-56).

As per claim 26, Wiegley teaches of a method of sending a document file for printing by a specified authorized recipient printing device, said method comprising the steps of selecting a content of said document file; encrypting said content; attaching a unique device identifier data, identifying a recipient device to which said document file is to be sent; and sending said document file to said recipient device (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 27, Wiegley discloses the step of adding a permitted quantity data to said document file, said permitted quantity data specifying a permitted number of copies of said document file which can be printed (col. 4, lines 30-46).

As per claim 28, the teachings of Wiegley disclose of the steps of storing a document history data, said document history data specifying for said document file a list of at least one recipient device to which said document file may be sent; a number of permitted copies of said document file which are permitted to be printed by each said recipient device (col. 4, lines 30-46).

As per claim 29, it is taught by Wiegley of a computer entity comprising a data processor, a data storage device, a printer port, and having an attached printer device, said computer entity comprising: a module for decrypting an encrypted document file; a unique device identifier for identifying said computer entity; wherein said computer entity operates to receive a document file in encrypted format; decrypt said document; extract a unique device identifier data from said document; compare said extracted

unique identifier data with said unique device identifier of said computer entity; if a match is found between said received unique device identifier data of said document and said unique identifier of said computer entity, send a said document file for printing by said attached printer device; and after sending said document to said printer device, delete said document file from said computer entity (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 30, Wiegley discloses of a method of secure printing of a received document file, said method comprising the steps of receiving said document file in encrypted format; reading a unique device identifier data identifying a recipient device for which said document file is intended; comparing said unique device identifier data with a locally stored identifier data corresponding to a local computer entity device; if said locally stored identifier data differs from said unique device identifier data identifying said recipient device for which said document file is intended, deleting said document file without printing any physical copies of said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 31, Wiegley teaches of a method of secure printing of a received document file, said method comprising the steps of: receiving said document file in encrypted format; reading a unique device identifier data identifying a recipient device for which said document file is intended; comparing said unique device identifier data with a locally stored device identifier data; reading a permitted quantity data describing a permitted quantity of copies of said document file; and if said received unique device identifier data corresponds with said locally stored device identifier data, printing said

permitted quantity of copies of said document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 32, Wiegley discloses of a printer device comprising: a data input device for receiving an encrypted digital document file; a decryption algorithm for decrypting said received document file; a controller for controlling printing of an image of data contained in said received document file; and a printer mechanism for printing a physical copy of said document file, wherein said printer device locally stores a decryption key for operating said decryption algorithm to decrypt said received document file (col. 1, line 60 through col. 2, line 13 and col. 2, lines 35-53).

As per claim 33, it is taught by Wiegley of a printer device comprising a data input device for receiving a digital document file; a controller for controlling printing of an image of data contained in said received document file; and a printer mechanism for printing a physical copy of said document file, wherein said controller operates to compare a received unique identifier data contained in said received document file with a locally stored unique device identifier data stored at said printer device; if said received unique identifier data matches said stored unique device identifier, control printing of at least one said physical copy of said document file; and if said received unique identifier data contained the said received document file does not match said stored unique device identifier data, to inhibit printing of any physical copies of said document file (col. 1, line 60 through col. 2, line 13; col. 2, lines 35-53; and col. 3, lines 50-56).

As per claim 34, it is disclosed by Wiegley that the controller operates to control printing of a predetermined quantity of said physical copy, wherein said predetermined quantity is specified in said received document file (col. 4, lines 30-46).

As per claim 35, Wiegley teaches of a printer device comprising a data input device for receiving an encrypted digital document file; a decryption algorithm for decrypting said received document files; a controller for controlling printing of an image of data contained in said received document file; and a printer mechanism for printing a physical copy of said document file, wherein a decryption key is stored locally in said printer device for operating said decryption algorithm to decrypt said received document files; said controller operates to compare a received unique identifier data contained in said received document file with a locally stored unique device identifier data stored at said printer device; if said received unique identifier data matches said stored unique device identifier, control printing of at least one said physical copy of said document file; and if said received unique identifier data contained the said received document file does not match said stored unique device identifier data, to inhibit decryption of said document file and inhibit printing of any physical copies of said document file (col. 1, line 60 through col. 2, line 13; col. 2, lines 35-53; and col. 3, lines 50-56).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131

9/27/05

CR

September 27, 2005